POLITYKA BEZPIECZEŃSTWA W RELACJACH Z PODMIOTAMI ZEWNĘTRZNYMI

Numer referencyjny dokumentu: 1.2

SPIS TREŚCI

§ 1
WSTĘP

1. Zgodnie z § 17 *Polityki bezpieczeństwa Informacji Urzędu Marszałkowskiego Województwa Pomorskiego – dokument główny*, wprowadza się do stosowania *Politykę bezpieczeństwa w relacjach z podmiotami zewnętrznymi*.
2. Relacje z podmiotami zewnętrznymi w UMWP mają charakter sformalizowany, a współpraca odbywa się w oparciu o obowiązujące przepisy prawa, *Politykę Bezpieczeństwa Informacji Urzędu Marszałkowskiego Województwa Pomorskiego – dokument główny*, niniejszą *Politykę* oraz indywidualne umowy i porozumienia z ww. podmiotami.
3. Rejestry zawartych umów i porozumień prowadzone są w poszczególnych komórkach organizacyjnych UMWP przez ich kierowników lub osoby przez nich wyznaczone.
4. Umowy powierzenia danych osobowych ewidencjonowane są w rejestrze umów, prowadzonym w DAZ, za wyjątkiem umów o dofinansowanie projektów finansowanych ze środków unijnych.
5. Celem zapewnienia ochrony aktywów informacyjnych udostępnianych usługodawcom, dostawcom i innym osobom oraz podmiotom zewnętrznym wykonującym czynności w imieniu i na rzecz UMWP i/lub mającym dostęp do aktywów Urzędu, wprowadza się niniejsze zasady i wymogi bezpieczeństwa w zakresie współpracy z ww. osobami i podmiotami.
6. Przedmiotowe zasady i wymogi dot. w szczególności:
   1) udostępniania aktywów informacyjnych oraz monitorowania i kontroli dostępu,
   2) przestrzegania określonych zasad i wymogów przez podmioty zewnętrzne,
   3) obowiązków podmiotów zewnętrznychw zakresie zapewnienia ochrony aktywów informacyjnych UMWP,
   4) zgłaszania przypadków naruszenia lub podejrzenia naruszenia bezpieczeństwa informacji,
   5) uświadamiania pracowników podmiotów zewnętrznych w zakresie bezpieczeństwa informacji,
   6) postępowania z poufnymi informacjami, w tym powierzonymi podmiotom zewnętrznym danymi osobowymi.
7. Jednoczesnie zapisy niniejszej *Polityki* stanowią punkt wyjścia do indywidualnych ustaleń i zapisów uzupełniających w umowach lub porozumieniach z podmiotami zewnętrznymi, których zakres zależy od charakteru i specyfiki współpracy.
8. W przypadku wykonywania zadań delegowanych i/lub korzystania z aktywów, w tym przetwarzania informacji powierzonych przez podmioty zewnętrzne w drodze stosownej umowy lub porozumienia, poza wymogami określonymi w obowiązującej w UMWP dokumentacji bezpieczeństwa, dopuszcza się stosowanie dodatkowych wymogów bezpieczeństwa określonych przez ww. podmioty zewnętrzne, o ile wskazane wymogi *„zewnętrzne”* nie obniżają poziomu bezpieczeństwa informacji przetwarzanych w UMWP.
9. Zapisy niniejszego dokumentu mają charakter uzupełniający do treści *Polityki Bezpieczeństwa Informacji Urzędu Marszałkowskiego Województwa Pomorskiego - dokument główny oraz* dokumentów II i III poziomu SZBI, tworząc wspólnie kompleksową dokumentację bezpieczeństwa informacji przetwarzanych w UMWP.
10. Niniejsza *Polityka bezpieczeństwa w relacjach z podmiotami zewnętrznymi* podlega przeglądom pod kątem aktualności, przydatności i adekwatności, zgodnie z zasadami monitorowaniai aktualizacji dokumentacji bezpieczeństwa określonymi w *Polityce monitorowania i nadzoru nad bezpieczeństwem informacji*.

§ 2
WYKAZ SKRÓTÓW I DEFINICJI

1. Stosowany w treści niniejszej *Polityki* termin „podmiot zewnętrzny” (m.in. wykonawcy i kontrahenci, dostawcy produktów, materiałów i usług) oznacza wszystkich pracowników tego podmiotu, wykonujących czynności w imieniu i na rzecz UMWP i/lub mających dostęp do aktywów Urzędu w związku z realizacją zawartej umowy lub porozumienia.

2. Pozostałe stosowane w niniejszej *Polityce* definicje i skróty należy rozumieć zgodnie z *Wykazem podstawowych skrótów i definicji*, stanowiącym załącznik nr 1 do *Polityki Bezpieczeństwa Informacji Urzędu Marszałkowskiego Województwa Pomorskiego – dokument główny.*

§ 3

ZAKRES STOSOWANIA

1. Niniejsza *Polityka bezpieczeństwa w relacjach z podmiotami zewnętrznymi* określa zasady i wymogi oraz tryb współpracy z podmiotami zewnętrznymi, w tym współpracy w obszarze dostaw technologii informacyjnych i telekomunikacyjnych.
2. Wykonawca będący stroną zawartej umowy lub porozumienia zobowiązany jest do zapoznania podległych mu pracowników realizujacych przedmiot ww. umowy lub porozumienia z zasadami ochrony aktywów informacyjnych Urzędu Marszałkowskiego Województwa Pomorskiego (UMWP), określonymi w szczególności w *Polityce bezpieczeństwa informacji Urzędu Marszałkowskiego Województwa Pomorskiego – dokument główny* oraz niniejszej *Polityce bezpieczeństwa w relacjach z podmiotami zewnętrznymi.*
3. Pracownicy współpracujących podmiotów zewnętrznych, o których mowa w ust. 2 zobowiązani są do przestrzegania zasad ochrony aktywów informacyjnych określonych w ww. *Politykach*.

§ 4

PRZYZNAWANIE DOSTĘPU PODMIOTOM ZEWNĘTRZNYM DO AKTYWÓW INFORMACYJNYCH URZĘDU

1. Pracownicy podmiotów zewnętrznych, o których mowa w § 3, realizujący określone zadania na podstawie zawartej umowy cywilnoprawnej lub porozumienia mogą otrzymać dostęp do aktywów informacyjnych Urzędu, w tym do:
   1) informacji sklasyfikowanych w poszczególnych grupach:
      a) dane osobowe,
      b) tajemnice prawnie chronione,
      c) tajemnice Urzędu,
      d) informacje jawne,
   2) aktywów wspierających przetwarzanie ww. informacji:
      a) sprzęt (w tym komputery, nośniki informacji),
      b) oprogramowanie,
      c) sieć,
      d) personel (w tym pracownicy UMWP),
      e) lokalizacja/siedziba (w tym pomieszczenia biurowe Urzędu),
      f) organizacja (w tym procedury wewnętrzne określające zasady i tryb funkcjonowania poszczególnych struktur organizacyjnych Urzędu),

w ograniczonym zakresie, niezbędnym do realizacji zleconych prac.

2. Przyznawanie, zmiana, ograniczenie i odbieranie praw dostępu do aktywów informacyjnych podmiotom zewnętrznym odbywa się zgodnie z obowiązującymi przepisami prawa, na formalny wniosek właściwego kierownika komórki organizacyjnej, odpowiedzialnego za przygotowanie i/lub relizację umowy lub porozumienia, na zasadach i w trybie określonym w *Polityce kontroli dostępu* i treści *dedykowanych polityk dla poszczególnych grup informacji*.
3. Przyznawanie rozszerzonych uprawnień do aktywów informacyjnych lub dodatkowych przywilejów możliwe jest po przedłożeniu stosownego uzasadnienia przez ww. kierownika i po formalnym odnotowaniu przedmiotowej zmiany.
4. Dostęp zdalny podmiotów zewnętrznych do aktywów informacyjnych Urzędu, np. w związku z wykonywaniem prac serwisowych i aktualizacji przyznawany jest w zakresie niezbędnym do realizacji zadań wynikających z treści umowy lub porozumienia i tylko pod nadzorem uprawnionych pracowników Urzędu.

5. Zasady dostępu fizycznego do budynków i pomieszczeń UMWP dla podmiotów zewnętrznych:
   1) Pracownicy podmiotów zewnętrznych mają swobodny dostęp do ogólnodostępnej strefy bezpieczeństwa obejmującej wejścia do budynków UMWP, hole, korytarze oraz wybrane pomieszczenia nie stanowiące pomieszczeń ograniczonego dostępu i/lub podwyższonego poziomu bezpieczeństwa, w tym pomieszczenia użyteczności publicznej takie jak punkty obsługi klienta, sala konferencyjna, poczta, przedszkole, punkt gastronomiczny etc.
   2) Pracownicy podmiotów zewnętrznych mogą uzyskać dostęp do strefy administracyjnej (ograniczonego dostępu), w tym pomieszczeń biurowych, pomieszczeń, gdzie składowane są uszkodzone komputerowe nośniki danych oraz archiwum, punktów dostaw i załadunku, w zakresie wynikającym z realizacji zadań określonych w treści zawartych umów lub porozumień i na wniosek właściwego kierownika.
   3) W strefie o podwyższonym poziomie bezpieczeństwa obejmującej m.in. systemy serwerowe, pracownicy podmiotów zewnętrznych mogą przebywać tylko pod ścisłym nadzorem GASI lub ASI. Dostęp do strefy o podwyższonym poziomie bezpieczeństwa jest na bieżąco rejestrowany.

§ 5

PODSTAWOWE ZASADY BEZPIECZEŃSTWA W ZAKRESIE WSPÓŁPRACY Z PODMIOTAMI ZEWNĘTRZNYMI

1. W uzupełnieniu do zasad i wymogów określonych w *Polityce bezpieczeństwa informacji Urzędu Marszałkowskiego Województwa Pomorskiego – dokument główny*, podmioty zewnętrzne w ramach współpracy z Urzędem zobowiązane są przestrzegać niniejszych zasad bezpieczeństwa dot. przedmiotowej współpracy.
2. W przypadku korzystania z budynków i pomieszczeń UMWP, pracownicy podmiotów zewnętrznych zobowiązani są również do zapoznania i stosowania się do zapisów obowiązującej instrukcji przecipożarowej i przepisów BHP.
3. W uzasadnionych przypadkach mogą być prowadzone dodatkowe szkolenia dla pracowników podmiotów zewnętrznych z zakresu bezpieczeństwa informacji.
4. Ww. podmioty zobowiązane są jednocześnie stale troszczyć się o powierzone im aktywa informacyjne oraz zachować szczególną ostrożność przy bieżącym korzystaniu z tych aktywów, w szczególności zadbać o zabezpieczenie ich przed utratą, kradzieżą, nieuprawnioną modyfikacją, uszkodzeniami mechanicznymi poprzez stosowanie adekwatnych zabezpieczeń, w tym przestrzeganie „zasady czystego biurka” i „zasady czystego ekranu”.
5. Pracownikom podmiotów zewnętrznych nie wolno podejmować prób sprawdzania, testowania i omijania zabezpieczeń powierzonych im aktywów informacyjnych, w tym:
   1) samowolnie modyfikować ustawień związanych z bezpieczeństwem,
   2) świadomie wprowadzać błędnych danych,
   3) podejmować prób przywłaszczenia lub rozszyfrowania informacji uwierzytelniających innych użytkowników.
6. W ramach zapewnienia poufności informacji przetwarzanych w UMWP, pracownicy podmiotów zewnętrznych zobowiązani są zachować w tajemnicy przez czas nieokreślony (w trakcie jak i po zakończeniu trwania umowy lub porozumienia) informacje udostępnione im w związku z realizacją umowy lub porozumienia oraz chronić je przed ujawnienieniem osobom nieuprawnionym.
7. Wymóg zachowania poufności, o którym mowa w ust. 6 obejmuje wszelkie informacje, których ujawnienie mogłoby narazić UMWP na szkodę. Przedmiotowy wymóg nie dotyczy informacji, które:
   1) są jawne i/lub ogólnodostępne,
   2) UMWP przekazał podmiotowi zewnętrznemu z możliwością dalszego ujawnienia.
8. W trakcie trwania umowy lub porozumienia, podmiot zewnętrzny zobowiązuje się ponadto:
   1) do wykonania przedmiotu umowy lub porozumienia:
      a) zgodnie z wymogami prawa powszechnie obowiązującego i treścią zawartej umowy lub porozumienia,

b) z zachowaniem najwyższej profesjonalnej staranności i przy wykorzystaniu całej posiadanej wiedzy i doświadczenia,

c) przy wykorzystaniu wybranego personelu posiadającego niezbędną wiedzę i umiejętności,

d) w sposób niepowodujący zaprzestania lub zakłócenia ciągłości pracy Urzędu,

2) nie zapoznawać się z dokumentami, analizami, zawartością systemu i aplikacji, dysków twardych etc., które nie są związane z przedmiotem umowy lub porozumienia,

3) nie powielać powierzonych informacji w zakresie szerszym, niż jest to potrzebne dla realizacji przedmiotu umowy lub porozumienia, w tym nie kopiować informacji celem udostępnienia ich osobom nieuprawnionym.

9. Po zakończeniu przedmiotowej współpracy, podmiot zewnętrzny zobowiązany jest niezwłocznie, w zależności od decyzji Urzedu, zwrócić lub zniszczyć udostępnione aktywa, w tym sprzęt lub informacje przekazane mu na dowolnych nośnikach, włączając wszelkie ich kopie. Na pisemne polecenie Urzędu, fakt zwrotu aktywów, w tym informacji potwierdza się w formie pisemnego protokołu przekazania. W przypadku zniszczenia aktywów, podmiot zewnętrzny zobowiązany jest złożyć pisemne oświadczenie potwierdzające dokonanie zniszczenia.
10. Dodatkowe zapisy dot. obowiązków podmiotów zewnętrznych wykonujących usługę ochrony i sprzątania w budynkach i pomieszczeniach UMWP określa dedykowana procedura DAZ na III poziomie SZBI, udostępniana wybranym pracownikom podmiotów zewnętrznych na „zasadzie wiedzy uzasadnionej".

§ 6

TREŚĆ UMÓW I POROZUMIEŃ Z PODMIOTAMI ZEWNĘTRZNYMI

1. Celem zmniejszenia ryzyk związanych z dostępem podmiotów zewnętrznych do aktywów UMWP, w treści zawieranych umów lub porozumień wprowadza się zapisy dotyczące bezpieczeństwa informacji, w tym klauzule bezpieczeństwa o zachowaniu poufności i nieujawniania informacji do których otrzymają dostęp, przyznanych praw i obowiązków oraz odpowiedzialności w zakresie bezpieczeństwa informacji, w tym tych, które pozostają wiążące po zakończeniu umowy.
2. W przypadku przetwarzania danych osobowych, powierzenie przetwarzania danych możliwe jest na podstawie umowy powierzenia zawartej zgodnie z obowiązującymi przepisami prawa dot. ochrony danych osobowych. Kierownik właściwej komórki organizacyjnej UMWP wprowadza stosowne zapisy dotyczące powierzenia przetwarzania danych osobowych, na zasadach określonych w *Polityce bezpieczeńsywa danych osobowych*.
3. W zależności od przedmiotu i specyfiki współpracy oraz zidentyfikowanych zagrożeń, poza wymogami wprost okreslonymi w obowiązujących przepisach prawa oraz dokumentacji bezpieczeństwa, o której mowa w § 3, w treści zawieranych umów lub porozumień (ewentualnie w aneksach do już istniejących umów lub porozumień) kierownik komórki organizacyjnej odpowiedzialny za ich przygotowanie wprowadza adekwatne zapisy uzupełniające dotyczące np.:

1) celu i zakresu przetwarzanych informacji,

1) osób upoważnionych do wymiany informacji i zatwierdzonych narzędzi komunikacji,

2) zakresu i poziomu świadczonych usług,

3) zasad i trybu postępowania w przypadku awarii lub katastrofy (czas reakcji, czas naprawy) i zapewnienia ciągłości świadczenia usług i dostaw,

4) akceptowalnego poziomu dostępności świadczonych usług (umowy SLA),

5) ochrony własności intelektualnej i praw autorskich oraz ich ewentualnego przeniesienia.

4. W uzasadnionych przypadkach, w tym z uwagi na potrzebę doskonalenia dostarczanych produktów i usług, wprowadzenia nowych wersji dokumentacji bezpieczeństwa, wprowadzenia nowych zabezpieczeń, zmiany lokalizacji, wprowadza się stosowne zmiany w już zawartych umowach lub porozumieniach. Przedmiotowe zmiany wprowadza się w formie aneksów do już istniejących umów lub porozumień.

§ 7

MONITOROWANIE I PRZEGLĄD USŁUG ŚWIADCZONYCH PRZEZ PODMIOTY ZEWNĘTRZNE

1. Dostęp podmiotów zewnętrznych i korzystanie z aktywów informacyjnych Urzędu przez ich pracowników są nadzorowane i monitorowane, m.in. za pośrednictwem systemu monitoringu wizyjnego (CCTV).
2. Bieżący nadzór nad udostępnianiem i korzystaniem z aktywów informacyjnych przez podmioty zewnętrzne prowadzi właściwy kierownik komórki organizacyjnej lub osoba/osoby przez niego wyznaczone.
3. Ww. kierownicy zobowiązani są również do monitorowania czy współpracujace podmioty zewnętrzne realizują swoje zadania zgodnie z prawem i treścią zawartych umów lub porozumień, a dostarczane przez nich produkty i usługi są zgodne z przedmiotem umowy lub porozumienia oraz funkcjonują zgodnie z oczekiwaniami.
4. Na wniosek UMWP, podmiot zewnętrzny zobowiązany jest niezwłocznie przekazać informacje dotyczące postępów prac, przyczyn opóźnień lub przyczyn nienależytego wykonywania zawartej umowy lub porozumienia. Informacje przekazywane są w formie pisemnej.
5. W uzasadnionych przypadkach, podmiot zewnętrzny zobowiązany jest umożliwić weryfikację postępów prac bezpośrednio w swojej siedzibie w formie postępowania sprawdzającego (audytu bezpieczeństwa).
6. Przedmiotowe zapisy dot. zasada monitorowania i przeglądu usług świadczonych przez podmioty zewnętrzne mogą zostać doszczegółowione w treści zawartych umów lub porozumień (ewentualnie w aneksach do już istniejących umów lub porozumień).

§ 8

ZGŁASZANIE PRZYPADKÓW NARUSZENIA BEZPIECZEŃSTWA INFORMACJI PRZEZ PODMIOTY ZEWNĘTRZNE

1. Pracownicy podmiotów zewnętrznych, zleceniobiorcy oraz inne osoby i podmioty zewnętrzne wykonujące czynności w imieniu i na rzecz UMWP i/lub mające dostęp do aktywów informacyjnych Urzędu, w przypadku zaistnienia okoliczności mogących świadczyć lub świadczących o naruszeniu bezpieczeństwa informacji w UMWP, zobowiązani są niezwłocznie poinformować o szczegółach i charakterze zdarzenia kierownika Referatu Bezpieczeństwa Informacji w Departamencie Organizacji (DO-B):
    a) Zgłoszenie do kierownika DO-B należy przesłać preferowanym kanałem: na *Formularzu zgłoszenia naruszenia bezpieczeństwa informacji*, którego wzór stanowi załącznik nr 1 do niniejszej *Polityki* - drogą mailową na adres incydent@pomorskie.eu.
    b) W uzasadnionych przypadkach dopuszcza się dokonanie przedmiotowego zgłoszenia w innym trybie np. telefonicznie na numer 58 326 85 18 lub 58 326 87 52.
2. Próby/przypadki nieautoryzowanego dostępu do aktywów informacyjnych UMWP są identyfikowane jako incydenty związane z bezpieczeństwem informacji.
3. Po powzięciu informacji o okolicznościach mogących świadczyć lub świadczących o naruszeniu bezpieczeństwa informacji, dalsze postępowanie, w tym obsługa i wyjaśnienie przyczyn incydentu związanego z bezpieczeństwem informacji, odbywa się zgodnie z *Procedurą obsługi i postepowania z incydentami związanymi z bezpieczeństwem informacji*, stanowiącą załącznik do *Polityki zarządzania incydentami związanymi z bezpieczeństwem informacji*.
4. Naruszenie postanowień umowy, porozumienia lub wymogów obowiązujacej dokumentacji bezpieczeństwa przez podmiot zewnętrzny stanowi podstawę do odstąpienia od umowy lub porozumienia i żądania pokrycia powstałej szkody lub zapłaty kary umownej, jeżeli taki obowiązek wynikał z zawartej umowy lub porozumienia.
5. Z tytułu działań podmiotów zewnętrznych i jego przedstawicieli, niezgodnych z przepisami prawa powszechnie obowiązującego (w tym dot. przetwarzania danych osobowych), grożą odrębne kary określone w szczególności w:
    1) kodeksie pracy,
    2) kodeksie cywilnym,
    3) kodeksie karnym,

4) RODO oraz ustawie o ochronie danych osobowych.

§ 9

ZASADY WSPÓŁPRACY Z PODMIOTAMI ZEWNĘTRZNYMI W PRZYPADKU NARUSZENIA BEZPIECZEŃSTWA INFORMACJI

1. Poza współpracą z tytułu zawartych umów i porozumień, z uwagi na wymogi prawa powszechnie obowiązującego, celem zapewnienia kompleksowej ochrony przetwarzanych informacji w UMWP, w tym ochrony przed cyberzagrożeniami, wymiany wiedzy i doświadczeń w obszarze bezpieczeństwa informacji oraz wsparcia procesu zarządzania zdarzeniami, w tym incydentami związanymi z bezpieczeństwem informacji, pracownicy UMWP współpracują z wybranymi instytucjami, organizacjami oraz podmiotami sektora publicznego i prywatnego.
2. W ramach przedmiotowej współpracy, w uzasadnionych przypadkach, w szczególności:
   1) w przypadku wybranych incydentów o priorytecie wysokim,
   2) w przypadku incydentów, które powodują lub mogą spowodować obniżenie jakości lub przerwanie realizacji zadania publicznego realizowanego przez podmiot publiczny,
   3) w przypadku incydentów noszących znamiona przestępstwa,

   informacja o incydencie przekazywana jest do właściwych podmiotów zewnętrznych, w tym:
   a) organów ścigania w przypadku incydentów wyczerpujących znamiona przestępstwa (np. przestępstwa przeciwko ochronie informacji wskazane w Kodeksie Karnym),
   b) Agencji Bezpieczeństwa Wewnętrznego,
   c) właściwych zespołów reagowania na Incydenty bezpieczeństwa komputerowego – w tym CSIRT NASK.
3. Współpraca z organem nadzorczym - Prezesem Urzędu Ochrony Danych Osobowych (dalej Prezes UODO) prowadzona jest w obszarze ochrony danych osobowych, w tym wymiany doświadczeń
   i stałego podnoszenia wiedzy pracowników UMWP.
4. Zgodnie z *RODO,* przypadki naruszenia ochrony danych osobowych prowadzącego do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych zostaną niezwłocznie zgłoszone organowi nadzorczemu, na zasadach i w trybie szczegółowo określonym w obowiązującej w UMWP *Procedurze obsługi i postępowania z incydentami związanymi z bezpieczeństwem informacji.*

FORMULARZ ZGŁOSZENIA NARUSZENIA BEZPIECZEŃSTWA INFORMACJI nr ……./rok[1]

1. Data i godzina zgłoszenia zdarzenia			
2. Źródło zgłoszenia[2]			
2.1 Imię i nazwisko Zgłaszającego			
2.2 Stanowisko		2.3 Numer telefonu/adres email (służbowy)	
2.4 Komórka organizacyjna UMWP[3]			
2.5 Nazwa podmiotu[4]			
2.6 Nazwa systemu monitorującego[5]			
2.7 Inne (jakie?)			
3. Opis potencjalnego naruszenia bezpieczeństwa informacji			
Proszę pokrótce opisać okoliczności (zdarzenia) wskazujące na naruszenie lub próbę naruszenia bezpieczeństwa informacji			

1 Uzupełnia kierownik DO-B lub osoba przez niego wskazana
2 Imię i nazwisko osoby/podmiotu zgłaszającego
3 W przypadku zgłoszeń z UMWP
4 W przypadku zgłoszeń od osób i podmiotów zewnętrznych wykonujących czynności w imieniu i na rzecz UMWP i/lub mających dostęp do aktywów informacyjnych Urzędu
5 W przypadku zgłoszeń z systemów monitorujących